NATIONAL FRAUD INTELLIGENCE BUREAU

MONTHLY THREAT UPDATE

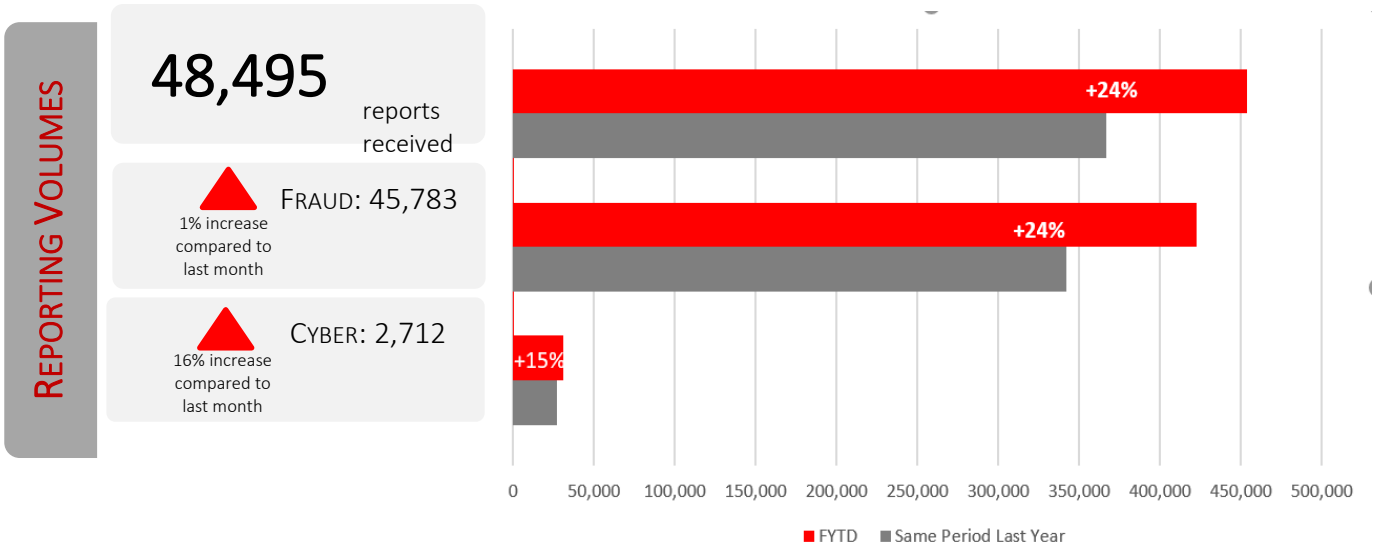
April 2021

Overview of Fraud and Cyber Dependant Crime Trends

CITY OF LONDON POLICE
National Policing Lead For Fraud

Fraud and Cyber Dependent Crime Trends

Action Fraud Crime Reporting Volumes In March 2021



- Reporting (crime and information reports) increased from 64,356 in February to 68,548 in March.
- Total losses dropped compared to the previous month from £286,562,188 in February to £275,192,021 in March. This represented an average loss of £4,003 per victim from £4,908 per victim.
- Dating fraud reporting continues to increase in volume (from 748 to 931) and as mentioned last month remains at its highest levels.
- Investment fraud reports continue to rise significantly in March, share sales have gone up to high levels again and Other Financial Investments have climbed and are now at the highest levels since reporting began.
- Online shopping fraud reporting has started to increase once more after a drop in reporting in February (from 8963 to 9386) whilst Mandate fraud[1] has increased to the highest levels since January 2020. Abuse of Position of Trust has increased once more after a drop in reporting last month to the highest levels since October 2020. Fraud Recovery continues to climb in volume and are now at the highest levels.
- Consumer Phone Fraud has continued to increase since it reached its highest levels in January. Ticket Fraud reports has increased again from the previous month (from 217 to 375 reports), likely due to the announcements around relaxations in restrictions. Door to Door Sales fraud is increasing once more and are now at its highest levels since September 2020.
- Rental Fraud reports have been rising since January after a steady drop in reporting in August. Lender Loan Fraud is increasing once more after a drop in figures in December. Application Fraud is now at the highest volume since February 2020. Telecoms Industry Fraud is now at its highest level since January 2020.
- After a drop in reporting last month, Computer Viruses and Malware reporting rose again to the highest figures since April 2020. Both Hacking – Server and Hacking Personal reporting showed increases with both at the highest levels. Hacking – Social Media reports has remained steady over the past few months.

Notable Reporting Trends

February's MO's: There has been a significant increase in delivery company branded smishing reported previously, with messages asking customers to click a link to either reschedule or pay for an underpaid delivery charge. There are a whole host of websites relating to package redelivery and delivery fees. There continues to be a significant number of suspect websites related to phishing scams involving text messages purporting to be from a bank stating that a new payee or new device has been added.

[1] Mandate Fraud is where fraudsters obtain details of direct debits, standing orders or account transfer details and amend them to transfer money to other accounts.

EMERGING ISSUES

Festival/Concert Ticketing Fraud: Other festivals/concerts have now been announced, including Leeds/Reading, Creamfields, Latitude, Camp Bestival, Wireless and Isle of Wight. There has been a huge demand for tickets with some festivals. Action Fraud have started to see reports of ticketing fraud and we would expect to see reports significantly increase over the coming months.

Holiday Fraud: NFIB have issued an alert to warn members of the public about the risk of holiday fraud and ticketing scams following the government's announcement of the road map out of lockdown. The Transport Secretary has recently been reported as saying that people can now think about booking foreign holidays[2] and Virgin are expecting a significant increase in demand over the coming months[3]. Any significant demands for holidays are likely to be exploited by scammers leading to an increase in holiday fraud.

False Address Registration: There has been an increase in the number of house owners reporting that they have received letters from Companies House confirming the registration of a company with the address showing as the house owners. At present it is not known what potential fraud may be carried out because of this false address registration.

EMERGING FRAUD THREATS

Easing of Lockdown Restrictions: As lockdown measures are eased, it is likely that we will see movement in volumes relating to certain fraud types. For example, volumes of reports relating to holiday scams and ticketing fraud are likely to increase once more. We may see a significant decrease in online shopping fraud as shops and services open once more, however, online buying behaviours may have changed because of the pandemic, therefore, online shopping scams may continue to be higher than prior to lockdown.

Covid Testing for Holidaymakers: One of the big barriers to international travel is likely to be the cost of tests for holiday makers to prove they are Covid negative. It is likely that private testing systems offering this service at low costs are likely to be overwhelmed by the sheer demand for tests. Other companies may prove too expensive, and fraudsters may look to take advantage of this demand by purporting to offer reasonably priced tests to holidaymakers.

Post-Vaccine Survey Scams: The Intellectual Property Rights Centre has warned that an increasing number of victims are being contacted via email and/or text message after receiving the COVID19 vaccine and being asked to participate in a fraudulent post-vaccine survey with the promise of a prize or cash at the end. Their credit card information is requested, and they are charged for the shipping and handling fees, but never receive the promised prize. Although the victims appear to be based in the US at present, it is likely that we could see reports in the UK.

COVID-19 19 Vaccine and Testing Certificates: Any potential databases containing details of vaccinated individuals are susceptible to cyber-attacks, hacking and data theft.

End of Furlough Schemes: It is highly likely that following the end of the furlough scheme is September, there will be an increase in demand for short term loans with fraudsters likely to exploit this demand and advance fee frauds will increase as a result. There is likely to be an increase the volume of cold calls from companies purporting to offer various loans to individuals struggling financially.

Permanent Home Working: Even as lockdown eases and more individuals are vaccinated, it is likely that a high number of individuals will continue to work from home either on a full time or part time basis. This will mean remote working will continue to be exploited by both cyber criminals and fraudsters.

[2] COVID-19: People can now think about booking foreign holidays, says transport secretary | UK News | Sky News

[3] COVID-19: Virgin Atlantic boss expecting increased demand for air travel in coming months | Business News | Sky News